

INFORMATION DISCLOSURE
CITATION IN AN APPLICATION
(PTO-1449)

ATTY. DOCKET NO.

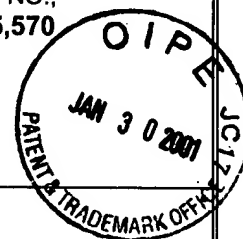
50325-0512
RECEIVED

SERIAL NO.,

09/675,570

FEB - 5 2001

TC 2100 MAILROOM



APPLICANT

David MCGREW, et al.

FILING DATE

September 29, 2000

GROUP

2132

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE


FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

DL	O. Goldreich et al., "How to Construct Random Functions," Journal of the Association for Computing Machinery, 53:4 (October, 1986), pp. 792-807.
EXAMINER	DATE CONSIDERED
Jm	3/30/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION  (PTO-1449)				ATTY. DOCKET NO. 50325-0512		SERIAL NO. 09/675,570			
				APPLICANT David McGrew, et al.				RECEIVED MAR 01 2002	
				FILING DATE September 29, 2000		Technology Center 2100 2132			
U.S. PATENT DOCUMENTS									
EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE			
JL	5,454,039	9/26/95	Coppersmith et al.	380	28	12/6/93			
JL	5,675,652	10/7/97	Coppersmith et al.	380	28	6/7/95			
JL	5,835,597	11/10/98	Coppersmith et al.	380	28	3/31/97			
FOREIGN PATENT DOCUMENTS									
EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation			
						Yes	No		
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)									
JL	B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," 2 nd ed. (New York: John Wiley & Sons, 1996), pp. 400-402								
JL	Rogaway, P. and Coppersmith, D., "A Software-Optimized Encryption Algorithm", Proc. of 1994 Fast Software Encryption Workshop, Lecture Notes In Computer Science, Vol. 809, Springer-Verlag, 1994, pp. 56-63, <i>reprinted in</i> J. Cryptology 11:4, Springer-Verlag, 1998, pp. 273-287, <i>and</i> http://www.cs.ucdavis.edu/~rogaway/papers/seal-abstract.html .								
JL	M. Bellare et al., "Forward Integrity for Secure Audit Logs," Dept. Comp. Sci. Eng., Univ. Calif. at San Diego, Nov. 23, 1997.								
JL	B. Schneier et al., "Cryptographic Support for Secure Logs on Untrusted Machines," Proc. Seventh USENIX Security Symposium, USENIX Press, Jan. 1998, pp. 53-62.								
JL	S. Kent et al., "Security Architecture for the Internet Protocol," IETF Request for Comments (RFC) 2401, The Internet Society, Nov. 1998.								
JL	S. Kent et al., "IP Authentication Header," IETF Request for Comments (RFC) 2402, The Internet Society, Nov. 1998.								
JL	S. Kent et al., "IP Encapsulating Security Payload (ESP)," IETF Request for Comments (RFC) 2406, The Internet Society, Nov. 1998.								
JL	D. Harkins et al., "The Internet Key Exchange (IKE)," RFC 2409, The Internet Society, Nov. 1998								
JL	H. Orman, "The OAKLEY Key Determination Protocol," RFC 2412, The Internet Society, Nov. 1998.								
EXAMINER				DATE CONSIDERED					
Jm Jia				3/29/04					

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.